PATENT
B422-240 (25813.247)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Shinichi Yamazaki, et al.
Serial No.	:	10/640,607
For	:	COMMUNICATION SYSTEM AND MANAGEMENT APPARATUS AND METHOD FOR RESTRICTING FUNCTIONS IN COMMUNICATION SYSTEM
Filed	:	August 13, 2003
Examiner	:	Beemnet W. Dada
Art Unit	:	2135

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

CLAIM TO BENEFIT OF 35 U.S.C. § 119
AND FILING OF PRIORITY DOCUMENTS

Claim is made herein to the benefit of 35 U.S.C. § 119 of the filing dates of the following Japanese Patent Application Nos.: 2002-247899 (filed August 28, 2002) and 2003-189924 (filed July 2, 2003), certified copies of which are filed herewith.

Dated: February 23, 2007

Respectfully submitted,

John J. Torrente
Reg. No. 26,359
Attorney of Record

COWAN, LIEBOWITZ & LATMAN, P.C.
1133 Avenue of the Americas
New York, New York 10036-6799
Tel. (212) 790-9200

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on: February 23, 2007
John J. Torrente
Signature
February 23, 2007
Date of Signature

CFO/7702 US/sum

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年　８月２８日

出願番号
Application Number: 特願２００２－２４７８９９

[ST. 10/C]: [ＪＰ２００２－２４７８９９]

出願人
Applicant(s): キヤノン株式会社

２００３年　９月１６日

特許庁長官
Commissioner,
Japan Patent Office

今井康

出証番号　出証特２００３－３０７５５８８

【書類名】　特許願
【整理番号】　4675040
【提出日】　平成14年 8月28日
【あて先】　特許庁長官殿
【国際特許分類】　H04N　1/00
【発明の名称】　会議システムの管理サーバ
【請求項の数】　10
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　山▲崎▼　信一
【特許出願人】
【識別番号】　000001007
【氏名又は名称】　キヤノン株式会社
【代理人】
【識別番号】　100087446
【弁理士】
【氏名又は名称】　川久保　新一
【手数料の表示】
【予納台帳番号】　009634
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9704186
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　会議システムの管理サーバ

【特許請求の範囲】

【請求項１】　ネットワークを介して、会議に参加するユーザによって操作される複数の電子機器と、電子機器との間で、情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される会議システムの管理サーバにおいて、

認証手続きを行う際に用いる認証情報に基づいて、参加者の立場を判別する参加者判別手段を有することを特徴とする会議システムの管理サーバ。

【請求項２】　請求項１において、

上記複数の電子機器は、電子機器との間で情報を送受信する会議システムの管理サーバと、近距離無線通信方式で接続することを特徴とする会議システムの管理サーバ。

【請求項３】　請求項１または請求項２において、

上記参加者判別手段は、主催者と参加者とを判別する手段であり、

上記会議システムの管理サーバは、操作制限を行う操作制限テーブルを有するサーバであることを特徴とする会議システムの管理サーバ。

【請求項４】　請求項３において、

上記操作制限テーブルで制限される項目として、上記参加者判別手段が判別した主催者と参加者とについて、広域ネットワークへの接続制限の項目を含むことを特徴とする会議システムの管理サーバ。

【請求項５】　請求項４において、

接続された端末機器について、ＩＰアドレスを割り当てると同時に、ＩＰアドレステーブルを作成するＩＰアドレステーブル作成部を有することを特徴とする会議システムの管理サーバ。

【請求項６】　請求項５において、

上記ＩＰアドレステーブル作成部で作成されたＩＰアドレステーブルと、ネッ

トワークに接続されたゲートウェイが持つＩＰアドレステーブルとを、共有し、記憶するＩＰアドレス記憶部を有することを特徴とする会議システムの管理サーバ。

【請求項７】　請求項１～請求項６のいずれか１項において、

上記近距離無線通信は、Ｂｌｕｅｔｏｏｔｈであることを特徴とする会議システムの管理サーバ。

【請求項８】　ネットワークを介して、会議に参加するユーザによって操作される複数の電子機器と、電子機器との間で、情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される会議システムの管理サーバにおいて、

認証手続きを行う際に用いる認証情報に基づいて、上記認証手続を行った電子機器に対して上記会議システムにおける機能制限を割り当てることを特徴とする会議システムの管理サーバ。

【請求項９】　ネットワークを介して、会議に参加するユーザによって操作される複数の電子機器と、電子機器との間で、情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される会議システムにおいて、

認証手続きを行う際に用いる認証情報に基づいて、上記認証手続を行った電子機器に対して上記会議システムにおける機能制限を割り当てることを特徴とする会議システム。

【請求項１０】　請求項１～請求項９のいずれか１項において、

上記認証情報は、ＢｌｕｅｔｏｏｔｈにおけるＰＩＮコードであることを特徴とする会議システムの管理サーバ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、会議システムに係り、特に、会議システムの参加者の立場の判断、および会議システムにおける機能制限の割り当に関する。

【０００２】

【従来の技術】

従来の会議では、紙ベースで発表資料を参加者全員に配布しているので、資源が無駄であるという問題があり、また、資料が人数分揃わない場合には、不足部数を慌ててコピーし、会議の進行を妨げるという問題がある。

【０００３】

ところで、近年は、発表者が、ＰＣやＰＤＡを、会議室に持ち込み、プロジェクタで投影し、プレゼンテーションするのが一般である。さらに、発表者以外の参加者にも、紙ベースではなく、ネットワーク経由で、資料データを配布することによって、上記問題が解決されている。

【０００４】

しかし、参加者が多い会議で、全員がネットワークを使用すると、配線が複雑になるという新たな問題が生じる。そこで、ＢｌｕｅＴｏｏｔｈ等の無線通信を用いた会議システムが考えられている。

【０００５】

ＢｌｕｅＴｏｏｔｈ方式は、アドホックなマルチポイント接続を行うので、最大接続数が、８機器、通信範囲が１０ｍのピコネットを構築し、通信することができ、通信速度に関しては、非同期通信において、下り７２１Ｋｂｐｓ、上り５７．６Ｋｂｐｓの通信が行える。また、音声通信もサポートし、１つのチャネルで、音声とデータとを転送することができる等、多種多様なプラットフォームでの利用が期待されている。

【０００６】

上記ＢｌｕｅＴｏｏｔｈ等の無線通信を用いた会議システムによって、配線の煩雑さは解消されるが、無線接続による外部からの不正アクセス、データの改ざん等セキュリティ面で、別の問題が浮上している。しかも、一度認証を通ってしまうと、資料のコピー、プリントアウト、データの上書き等の制限は、ＢｌｕｅＴｏｏｔｈの認証レベルでは実行することができない。

【０００７】

これに対して、特開２００１－３１２４７２公報では、異なる２種類のＰＩＮコードを用いて認証することによって、セキュリティレベルを向上する方法が提案されている。また、特開２００１－３３１４３１公報では、会議中の権限を、各端末に指定し、機能を制限することが提案されている。

【０００８】

【発明が解決しようとする課題】

特開２００１－３３１４３１公報では、参加者の機器に権限を与える際に、会議システムのアプリケーション上から、各参加者がタブを選択し、権限を設定する方法をとっている。

【０００９】

しかし、このようにすると、参加者の手間がかかる上、任意に権限の設定を変更することができ、権限を故意に変えてデータを操作することも可能であるという問題がある。

【００１０】

本発明は、会議システムのデータの不正な改ざんや情報の漏洩を防ぎ、しかも、機能制限をアプリケーション上で別個に行う手間を省くことを目的とするものである。

【００１１】

【課題を解決するための手段】

本発明は、ネットワークを介して、会議に参加するユーザによって操作される複数の電子機器と、電子機器との間で、情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される会議システムの管理サーバにおいて、認証手続きを行う際に用いる認証情報に基づいて、参加者の立場を判別する参加者判別手段を有することを特徴とする会議システムの管理サーバを提供する。

【００１２】

また、本発明は、ネットワークを介して、会議に参加するユーザによって操作

される複数の電子機器と、電子機器との間で、情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される会議システムの管理サーバにおいて、認証手続きを行う際に用いる認証情報に基づいて、上記認証手続を行った電子機器に対して上記会議システムにおける機能制限を割り当てることを特徴とする会議システムの管理サーバを提供する。

【００１３】

また、本発明は、ネットワークを介して、会議に参加するユーザによって操作される複数の電子機器と、電子機器との間で、情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される会議システムにおいて、認証手続きを行う際に用いる認証情報に基づいて、上記認証手続を行った電子機器に対して上記会議システムにおける機能制限を割り当てることを特徴とする会議システムを提供する。

【００１４】

【発明の実施の形態および実施例】

［第１実施例］

図１は、本発明の第１実施例である無線通信装置ＷＣ１を示すブロック図である。

【００１５】

無線通信装置ＷＣ１は、会議システム管理サーバ１０１と、アクセスポイント１０２と、ゲートウェイ１０３と、ＰＣまたはＰＤＡ１０４とを有する。

【００１６】

ＰＣまたはＰＤＡ１０４は、主催者や参加者が持参したＢｌｕｅｔｏｏｔｈによる無線接続が可能なＰＣまたはＰＤＡである。

【００１７】

会議システム管理サーバ１０１は、広域ネットワークへアクセスするために必要であり、会議システムのアプリケーションを動作させるサーバである。

【００１８】

アクセスポイント１０２は、無線端末から根幹のＬＡＮに接続する際に必要と

なるポイントである。また、アクセスポイントは、根幹のＬＡＮに接続され、一般的なスイッチングハブのような役目をする。持参したＰＣやＰＤＡを有線で会議サーバに接続する場合、ハブを用いて会議システム管理サーバ１０１に複数台接続することができるが、無線接続する場合は、各機器をアクセスポイントに接続し、会議システム管理サーバ１０１との間で、データをやりとりする。

【００１９】

アクセスポイント１０２へ接続する場合、セキュリティを考慮し、ユーザ認証の手続きを行う必要がある。一般的に、ＰＩＮコード（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）を交換することによって、ユーザ認証するが、アクセスポイントのデフォルトＰＩＮコードが固定であると、一度接続したことのある人なら、何度でも接続でき、セキュリティ面で問題がある。

【００２０】

そこで、会議の主催者が、予めデフォルトＰＩＮコードで、アクセスポイント１０２に接続し、会議の時にのみ有効なＰＩＮコードに変更する方法が採られている。

【００２１】

しかし、デフォルトＰＩＮコードが固定であると、誰でも設定を変更できるので、デフォルトＰＩＮコードを故意に変更することもできる。すると、正規の主催者が、会議の時にのみ有効なＰＩＮコードに変更しようと考え、固有のデフォルトＰＩＮコードで接続しても、接続できないという事態が生じる。

【００２２】

そこで、会議室予約システム等で会議室を予約した時に、その会議室付属のアクセスポイント１０２のデフォルトＰＩＮコードが設定され、同時に、主催者にメール等で通知し、主催者は、会議予約システム１０１から通知されたＰＩＮコードを使ってアクセスポイント１０２に接続し、会議の時にのみ有効なＰＩＮコードに変更する手段がとられている。参加者は、主催者から予め通知された会議の時にのみ有効なＰＩＮコードを含む参加証を持って、会議室に臨み接続する。

【００２３】

図２は、上記実施例における会議システム管理サーバ２０１を示すブロック図

である。

【００２４】

会議システム管理サーバ２０１は、主制御部２０２と、ネットワーク通信部２０３と、記憶部２０４と、入力部２０６と、表示部２０７と、テーブル作成部２０８と、判別部２０９と、データベース２０５とを有する。

【００２５】

ネットワーク通信部２０３は、主制御部２０２の指示に従い、有線通信網、無線通信網に接続される各種無線端末１０４との間で、データを送受信する。

【００２６】

主制御部２０２は、会議システム制御、各種アプリケーションの管理、入力部、表示部を制御し、記憶部２０４は、テーブル作成部２０８で作成された各種テーブルデータやファイル管理を行う。

【００２７】

入力部２０６は、キーボード、マウス等によって入力を制御し、表示部２０７は、ＣＲＴモニタ等の表示を制御する。テーブル作成部２０８は、ＩＰアドレステーブルや機能制限テーブル等各種テーブルを作成する。判別部２０９は、ネットワーク通信部２０３によって取得した参加証から、会議の主催者であるか、参加者であるかを判別する。

【００２８】

図３は、上記実施例において、会議の主催者が会議に参加するまでの動作を示すフローチャートである。

【００２９】

まず、会議の主催者は、会議室予約システム等で会議室の予約を行い（Ｓ３０１）、会議の時にのみ有効なＰＩＮコードに、設定を変更し（Ｓ３０２）、ＰＩＮコードを、会議の参加者に電子メール等で通知する（Ｓ３０３）。

【００３０】

次に、メールアドレス、ＰＩＮコード、社員ＩＤ等が記されている参加証ファイルを作成し（Ｓ３０４）、この作成したファイルを、参加者全員にそれぞれ配布し（Ｓ３０５）、会議に参加する（Ｓ３０６）。

【００３１】

図４は、上記実施例において、会議の参加者が会議に参加するまでの動作を示すフローチャートである。

【００３２】

まず、主催者が配布した会議の時にのみ有効なＰＩＮコードを、参加者が取得する（Ｓ４０１）。このときに、電子メールのみでなく、主催者が作成したＷｅｂ等にアクセスして、主催者が配布した会議の時にのみ有効なＰＩＮコードを取得するようにしてもよい。

【００３３】

次に、主催者が配布した参加証を、参加者が受け取り（Ｓ４０２）、参加者はその参加証を持参して、会議に参加する（Ｓ４０３）。この場合においても、参加証に、ＰＩＮコードが記載されているので、会議の時にのみ有効なＰＩＮコードを取得する処理（Ｓ４０１）を省くようにしてもよい。

【００３４】

図５は、上記実施例において、主催者がアクセスポイント１０２のＰＩＮコードを変更する処理を示すシーケンス図である。

【００３５】

まず、アクセスポイント１０２のデフォルトＰＩＮコードを、ＬＡＮに接続されたＰＣ等から設定する（Ｓ５０１）。このＰＣには、会議室予約システムが運用され、会議室予約システムは、会議室を予約した際に、自動的にＰＩＮコードが作成され、アクセスポイント１０２のデフォルトＰＩＮコードに設定し、同時に、予約者に通知するような機能を有する。

【００３６】

次に、主催者は、アクセスポイント１０２に、接続要求を発行する（Ｓ５０２）。アクセスポイント１０２は、接続要求を受け、データが正しければ、接続確立のメッセージを無線機器に送信し、接続が確立する（Ｓ５０３）。

【００３７】

その後に、アクセスポイント１０２が認証要求を発行し、パスワードの要求を促す（Ｓ５０４）。主催者側の端末は、会議室予約システム等で新たに設定され

たデフォルトＰＩＮコードを送信し（Ｓ５０５）、ＰＩＮコードが正しければ、アクセスポイントから認証完了が通知される（Ｓ５０６）。

【００３８】

次に、主催者側の端末が、ＰＩＮコードの設定変更要求を発行し（Ｓ５０７）、アクセスポイント１０２から、要求メッセージ受信応答が帰ってきたら（Ｓ５０８）、会議の時にのみ有効なＰＩＮコードを送信する（Ｓ５０９）。アクセスポイント１０２は、新たなＰＩＮコードを受信し、ＰＩＮコードの設定を変更し、変更完了のメッセージを主催者に送信し、接続処理が完了する（Ｓ５１０）。

【００３９】

図６は、上記実施例において、参加者が会議に参加する場合の処理を示すシーケンス図である。

【００４０】

参加者は、アクセスポイントに、接続要求を発行し（Ｓ６０１）、アクセスポイント１０２は、接続要求を受け、データが正しければ、接続確立のメッセージを無線機器に送信し、接続が確立する（Ｓ６０２）。

【００４１】

その後に、アクセスポイントが認証要求を発行し、パスワードの要求を促す。参加者の端末は、会議の時にのみ有効なＰＩＮコードを送信し（Ｓ６０４）、アクセスポイント１０２から認証完了のメッセージを受信したら（Ｓ６０５）、予め配布された参加証を、アクセスポイント１０２を経由して、会議システムに送信する（Ｓ６０６）。会議システムは、参加証を受信したら、受信応答を参加者の端末に送信し、接続処理が完了する（Ｓ６０７）。

【００４２】

図７は、上記実施例において、会議システム管理サーバの判別部２０９における動作を示すフローチャートである。

【００４３】

参加証には、最低限ＰＩＮコードが記述されていることを前提とし、参加証に記述されているＰＩＮコードが２種類（デフォルトＰＩＮコード、会議の時にのみ有効なＰＩＮコード）あり（Ｓ７０１）、しかも、会議システム管理サーバ１

０１が保持しているＰＩＮコードと一致すれば（Ｓ７０３）、接続相手を主催者と判別し、主催者としての機能権限を与える（Ｓ７０６）。

【００４４】

一方、ＰＩＮコードが１種類（会議の時にのみ有効なＰＩＮコード）であり（Ｓ７０１）、しかも、会議システム管理サーバ１０１が保持しているＰＩＮコードと一致すれば（Ｓ７０２）、参加者であると判別し、参加者としての機能権限を与える（Ｓ７０４）。不正なＰＩＮコードが記述された参加証を受信すれば、不正なアクセスとみなし、全ての操作を不能にする（Ｓ７０５）。

【００４５】

図８は、会議システムによって制限される機能のテーブルを示す図である。

【００４６】

［第２実施例］

上記会議システム管理サーバ１０１では、参加者それぞれにＩＰアドレスを割り当て、広域ネットワークへアクセスすることができるシステムが考えられる。しかし、この場合、参加者がＷｅｂのメールサービス等で重要な情報を故意に外部に漏らす可能性が考えられる。

【００４７】

本発明の第２実施例は、上記会議システム管理サーバ１０１が受信した参加証に、最低限ＰＩＮコードが記述されていることを前提に、参加証に記述されているＰＩＮコードによって、広域ネットワークへのアクセス制限をかける実施例である。

【００４８】

具体的には、上記会議システム管理サーバ１０１へ接続したときに取得する参加証に記載されているＰＩＮコードが、２種類（デフォルトＰＩＮコード、会議の時にのみ有効なＰＩＮコード）であり、しかも、会議システムが記憶し、保持しているデフォルトＰＩＮコード、会議の時にのみ有効なＰＩＮコードと一致すれば、主催者であると判別し、広域ネットワークへ接続できるＩＰアドレスを割り当てる。

【００４９】

ＰＩＮコードが、１種類（会議の時にのみ有効なＰＩＮコード）であり、しかも、正しいＰＩＮコードであれば、参加者であると判別し、広域ネットワークへ接続できないＩＰアドレスを割り当てる。会議システム管理サーバ１０１のＩＰアドレス取得方法は、ＬＡＮに接続されているゲートウェイ１０３が持つＩＰアドレステーブルを取得し、共有することで行う。

【００５０】

具体的には、無線端末１０４が会議システム管理サーバ１０１に接続したときに、会議システム管理サーバ１０１は、ゲートウェイ１０３が持つＩＰアドレステーブルを取得する。これと同時に、会議管理サーバが取得する参加証に記載されているＰＩＮコードに基づいて、主催者であるか、参加者であるかを判別し、広域ネットワークへのアクセスを許可できる無線端末に対してＩＰアドレスを配布する。

【００５１】

今回は、ゲートウェイが持つＩＰアドレステーブルの取得を、無線端末の接続と同時に行ったが、一定時間間隔テーブルを取得するようにしてもよい。

【００５２】

また、取得したＩＰアドレステーブルに、そのＩＰアドレスを追加し、ゲートウェイに送信することによって、ゲートウェイ１０３と会議システム管理サーバ１０１とで、ＩＰアドレステーブルを共有する。

【００５３】

第２実施例によれば、主催者と参加者とで広域ネットワークへのアクセス制限をかけることによって、不正な外部アクセスを防ぐことができる。

【００５４】

以上のように上記実施例によれば、予め電子メール等で配布される会議参加証に記載されているＰＩＮコードを用いて会議の参加者か主催者かを判別し、データのアクセス制限をかけることでデータの不正な改ざんを防ぐと共に制限の設定をアプリケーション上で別個に行う手間を省くことができるという効果を奏する。

【００５５】

【発明の効果】

以上のように本発明によれば、会議システムのデータの不正な改ざんや情報の漏洩を防ぎ、しかも、機能制限をアプリケーション上で別個に行う手間を省くことことができる。

【図面の簡単な説明】

【図１】

本発明の第１実施例である無線通信装置ＷＣ１を示すブロック図である。

【図２】

上記実施例における会議システム管理サーバ２０１を示すブロック図である。

【図３】

上記実施例において、会議の主催者が会議に参加するまでの動作を示すフローチャートである。

【図４】

上記実施例において、会議の参加者が会議に参加するまでの動作を示すフローチャートである。

【図５】

上記実施例において、主催者がアクセスポイント１０２のＰＩＮコードを変更する処理を示すシーケンス図である。

【図６】

上記実施例において、参加者が会議に参加する場合の処理を示すシーケンス図である。

【図７】

上記実施例において、会議システム管理サーバの判別部２０９における動作を示すフローチャートである。

【図８】

会議システムによって制限される機能のテーブルを示す図である。

【符号の説明】

ＷＣ１…無線通信装置、

１０１…会議システム管理サーバ、

１０２…アクセスポイント、

２０１…管理サーバ、

２０３…ネットワーク通信部、

２０４…記憶部、

２０５…データベース、

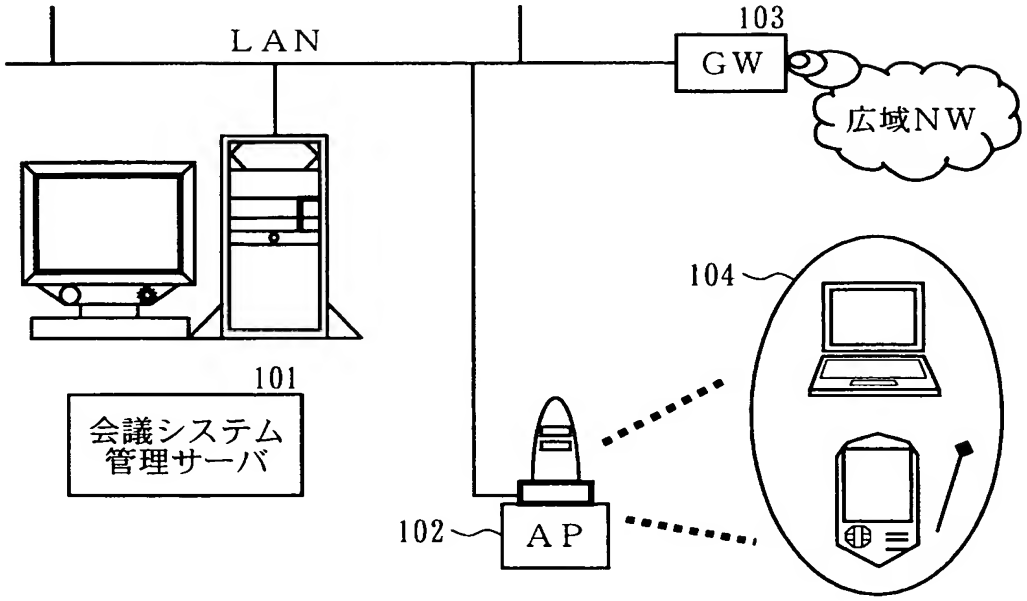
２０８…テーブル作成部、

２０９…判別部。

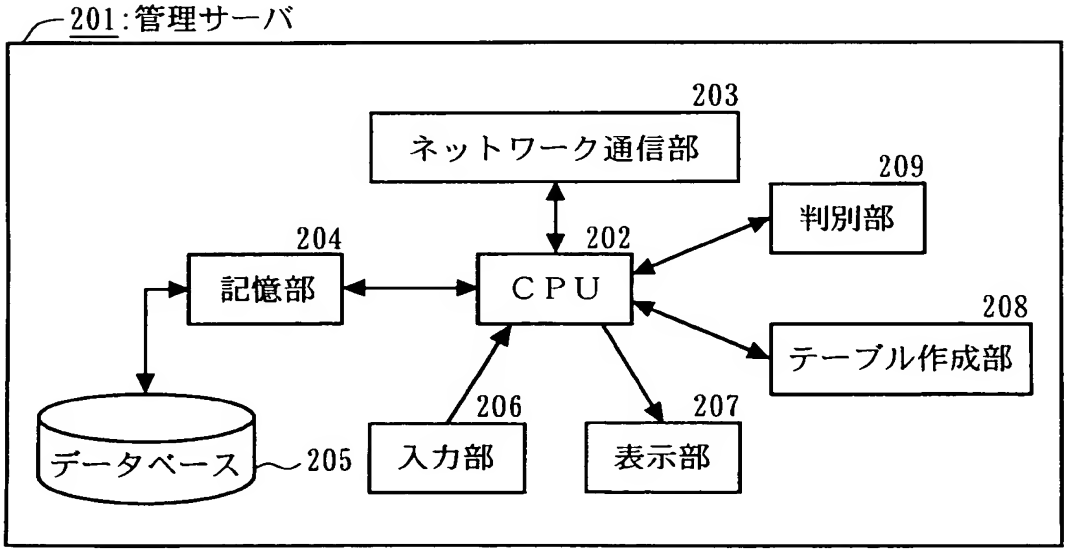
【書類名】　　図面

【図１】

WC１：無線通信装置



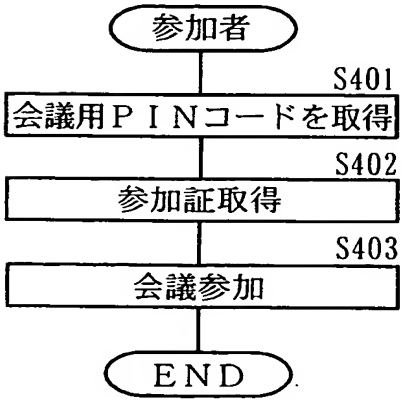
【図２】



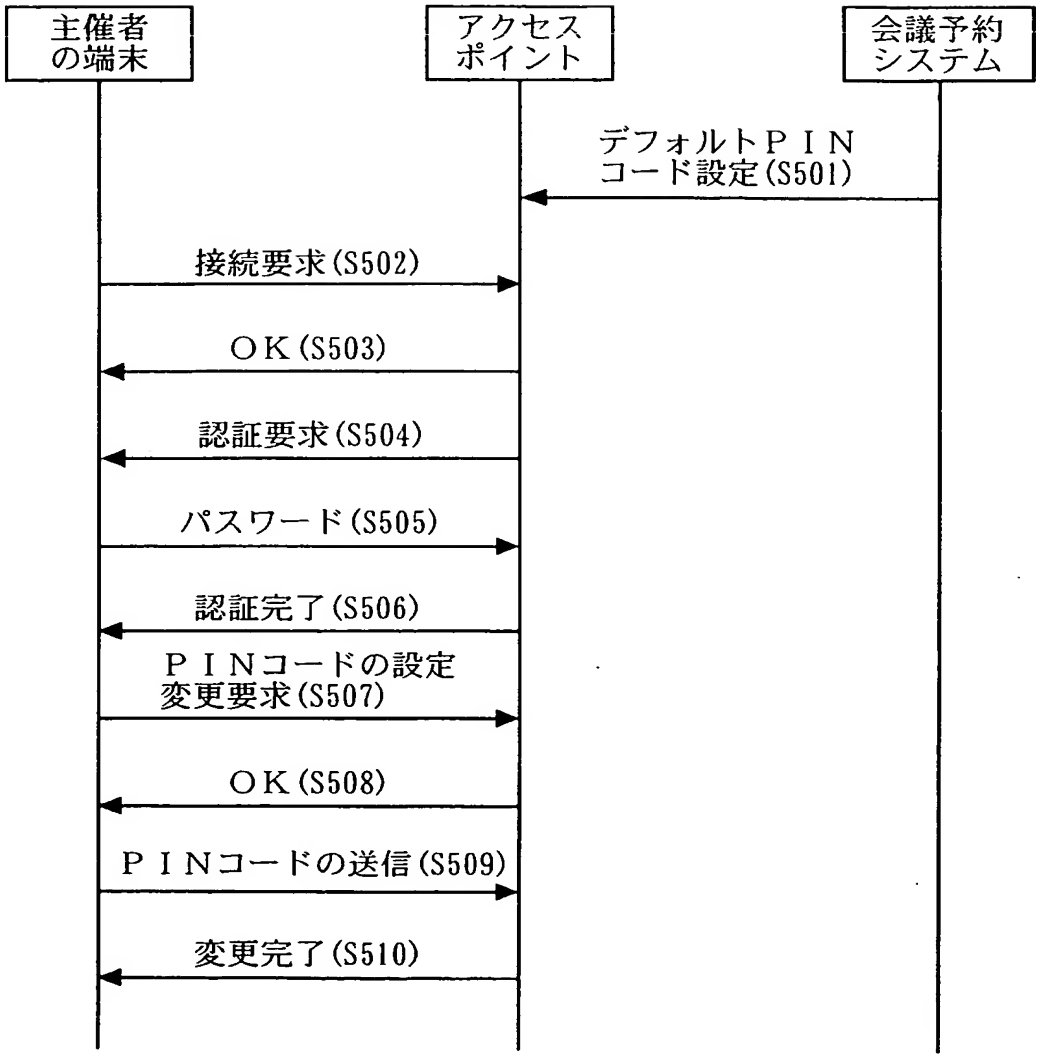
【図３】


主催者
S301
会議室予約
S302
ＰＩＮコードの設定変更
S303
変更したＰＩＮコードを参加者に通知
S304
参加証作成
S305
参加証配布
S306
会議参加
END

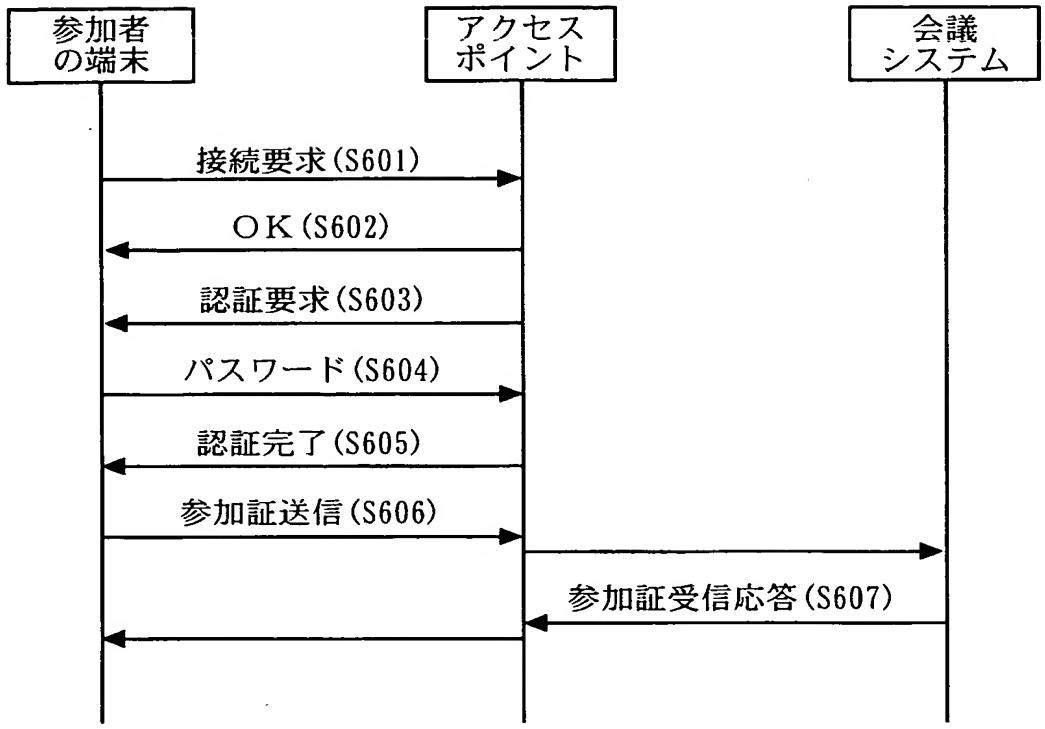
【図４】


参加者
S401
会議用ＰＩＮコードを取得
S402
参加証取得
S403
会議参加
END

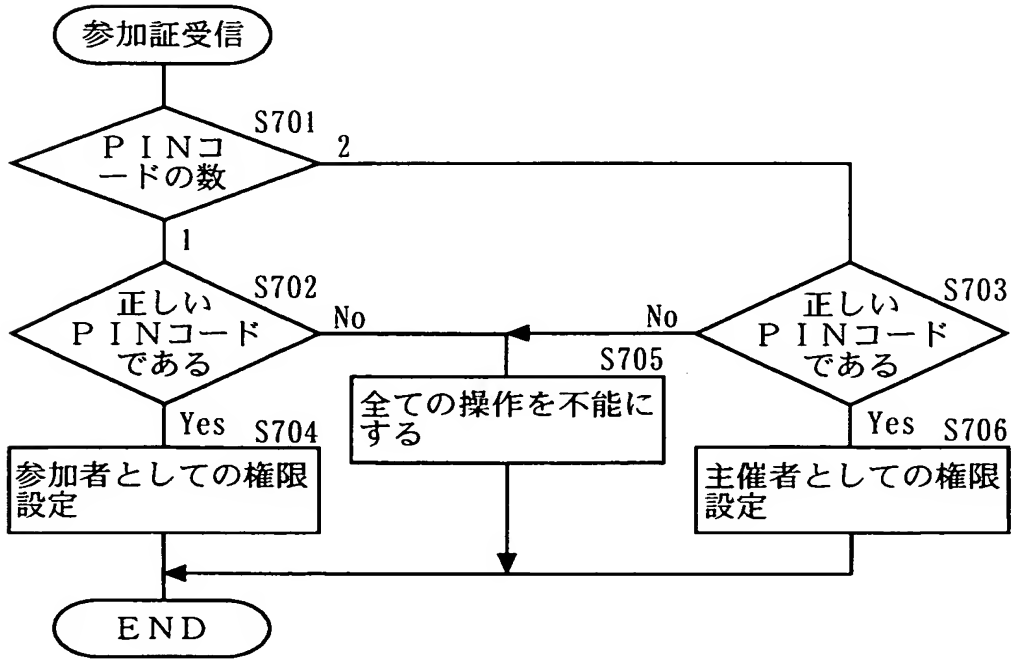
【図５】


主催者の端末
アクセスポイント
会議予約システム
デフォルトＰＩＮコード設定(S501)
接続要求(S502)
ＯＫ(S503)
認証要求(S504)
パスワード(S505)
認証完了(S506)
ＰＩＮコードの設定変更要求(S507)
ＯＫ(S508)
ＰＩＮコードの送信(S509)
変更完了(S510)

【図６】


参加者の端末
アクセスポイント
会議システム
接続要求(S601)
ＯＫ(S602)
認証要求(S603)
パスワード(S604)
認証完了(S605)
参加証送信(S606)
参加証受信応答(S607)

【図７】


参加証受信
S701
ＰＩＮコードの数
2
1
S702
正しいＰＩＮコードである
No
S703
正しいＰＩＮコードである
No
S705
全ての操作を不能にする
Yes
S704
参加者としての権限設定
Yes
S706
主催者としての権限設定
END

【図８】

機能	主催者	参加者
ファイルの閲覧	○	○
ファイルコピー	○	×
ファイル削除	○	×
ファイル印刷	○	×
ファイル名変更	○	×
ファイル上書き	○	×
ファイル保存	○	×
ネット閲覧	○	△
ＩＰアドレスの変更	○	×
ＰＩＮコードの変更	○	×
メール送受信	○	×

【書類名】　　要約書

【要約】

【課題】　会議システムのデータの不正な改ざんや情報の漏洩を防ぎ、しかも、機能制限をアプリケーション上で別個に行う手間を省くことができる会議システムの管理サーバを提供することを目的とするものである。

【解決手段】　ネットワークを介して、会議に参加するユーザによって操作される複数の電子機器と、電子機器との間で、情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される会議システムの管理サーバにおいて、認証手続きを行う際に用いる認証情報に基づいて、参加者の立場を判別する参加者判別手段を有することを特徴とする会議システムの管理サーバである。

【選択図】　図１

特願２００２－２４７８９９

出　願　人　履　歴　情　報

識別番号　　［０００００１００７］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都大田区下丸子３丁目３０番２号
氏　名　　キヤノン株式会社